**DRAFT DECREE ON PERSONAL DATA PROTECTION**

| GOVERNMENT | THE SOCIALIST REPUBLIC OF VIETNAM<br>Independence – Freedom – Happiness |
|---|---|
| No.: /2021/NĐ-CP | *Hanoi, ..... 2021* |

**2ND DRAFT**

# DECREE

## On personal data protection

*Pursuant to the Law on Organization of the Government dated June 19, 2015;*

*Pursuant to the Civil Code dated November 24, 2018;*

*Pursuant to the Law on National Security dated December 03, 2004;*

*Pursuant to the Law on Cyber Security dated June 12, 2018;*

*Pursuant to the Law on Handling of Administrative Violations dated November 13, 2020;*

*At the request of the Minister of Public Security,*

*The Government hereby promulgates a Decree on personal data protection,*

## Chapter I

## GENERAL PROVISIONS

### Article 1. Scope of governing and Subjects of application

1. This Decree governs personal data and processing thereof, measures for personal data protection, Personal Data Protection Commission, handling of personal data breaches; and responsibility for personal data protection of agencies, organizations and individuals.

2. This Decree applies to agencies, organizations and individuals involved in personal data.

### Article 2. Interpretation of terms

In this Decree, the terms below are construed as follows:

1. *Personal data* means data about individuals or relating to the identification or ability to identify a particular individual.

*2. Basic personal data* includes:

a) Surname name, middle name, and birth name, alias (if any);

b) Date of birth; date of death or date of going missing;

c) Blood type & gender;

d) Place of birth, place of birth registration, permanent residence, current residence, hometown, contact address, email address;

dd) Education;

e) Ethnicity;

g) Nationality;

h) Phone number;

i) ID card number, passport number, citizen identification number, driver's license number, plate number, personal tax identification number, social insurance number;

k) Marital status;

l) Data reflecting online activities or activity history.

3. *Sensitive personal data* includes:

a) Personal data on political and religious views;

b) Personal health data, i.e. information related to the physical or mental health status of the data subject collected and identified during the process of registration or provision of medical services;

c) Personal genetic data, i.e. information relating to inherited or acquired genetic characteristics of each individual;

d) Personal biometric data, i.e. information about physical and biological characteristics of each individual;

dd) Personal data on gender status, i.e. information about people identified as male, female, gender neutral, androgynous, or having both masculine and feminine characteristics or self-identifying a different gender from the gender identified at birth;

e) Personal data about life and sexual orientation;

g) Personal data about criminals and criminal acts collected and stored by law enforcement agencies;

h) Personal financial data, i.e. information used to identify an account,

card or payment instrument provided by a financial institution to a data subject or information about the relationship between a financial institution, original financial data and data subjects, including records, financial status, credit history, and income level;

i) Personal location data, i.e. information about the individual's previous and current physical location;

k) Personal data about social relationships;

l) Other personal data as specified by law to be special and subject to confidentiality protection.

4. *Personal data protection* means the prevention, detection, and handling of regulatory violations on personal data.

5. *Data subject* means any identifiable natural person to whom the personal data relates.

6. *Processing of personal data* means any action(s) to do with personal data, including collection, recording, analysis, storage, alteration, disclosure, granting of access to personal data, retrieval, recovery, encryption, decryption, copy, transfer, deletion, or destruction of personal data or other relevant actions.

7. *Right to personal data protection* means the individual's right to exercise or require agencies, organizations and individuals to respect, protect and take specific measures to protect his or her personal data.

8. ***Personal data processors*** mean domestic and foreign agencies, organizations and individuals engaged in processing personal data.

9. ***Third-parties*** mean domestic and foreign agencies, organizations and individuals allowed to receive personal data and engaged in some processing activities other than the personal data processors or data subjects.

10. *Automated processing of personal data* means the use of computer systems to make algorithmic decisions on personal data processing.

11. *Cross-border data transfer* means the use of cyberspace or electronic devices and means to transfer personal data of Vietnamese citizens to an area beyond the territory of the Socialist Republic of Vietnam.

12. *Original data* means the initial personal data processed by the processors and not yet transferred to a third party.

13. *Personal data de-identification* means the process of anonymizing or removing identifiers or replacing them with a pseudo name or other code to create new data that cannot identify a particular individual.

14. *Personal data anonymization* means the process of transforming

personal data into a new data that cannot be reversed into personal data.

15. *Regulatory violations on personal data protection* means any action that involves the unlawful processing of personal data.

**Article 3. Personal data protection principles**

1. *Lawfulness*: Personal data shall only be collected where necessary in accordance with the law.

2. *Purpose limitation*: Personal data shall only be collected for the purposes that have been consented or registered on personal data processing.

3. *Data minimization*: Personal data shall be limited to what is necessary in relation to specified purposes.

4. *Restricted use*: Personal data may be used only with the consent of the data subject or with the permission of the public authority in accordance with laws.

5. *Data quality*: Personal data must be adequately updated to achieve processing purposes.

6. *Security*: Personal data is subject to protective measures in the course of processing.

7. *Individuality*: Data subjects will be informed of all activities related to their personal data processing.

8. *Confidentiality*: Personal data must be kept confidential during data processing.

**Article 4. Handling of personal data breaches**

1. Agencies and organizations violating regulations on personal data protection, depending on the severity, may be sanctioned administratively or criminally, and subject to additional penalties specified by law.

2. The handling of personal data breaches is applied to all domestic and foreign organizations, enterprises and individuals doing business in Vietnam.

3. In addition to the specified fine level, repeated and material breaches by personal data processors may be subject to a fine of up to 5% of the personal data processor’s total revenues in Vietnam.

## Chapter II

## PERSONAL DATA PROCESSING

**Article 5. Rights of the data subjects to personal data processing**

1. Have the discretion to allow or not allow personal data processors or third parties to process their personal data, unless otherwise provided by law.

2. Receive notices from the personal data processors at the time of processing or as soon as possible.

3. Request the personal data processors to correct, view and provide a copy of their personal data.

4. Request the personal data processors to terminate the processing of personal data, restrict the right to access personal data, terminate the disclosure or access to personal data, delete or close collected personal data, unless otherwise specified by law.

5. File complaints in accordance with the law or complaints to the Personal Data Protection Commission in the following cases:

a) Their personal data is compromised;

b) Their personal data is processed for the wrong purposes and not in accordance with the agreement or the law;

c) Rights to their personal data are breached or not exercised properly.

6. Claim compensation in accordance with the law when there are grounds to believe that their personal data has been breached.

**Article 6. Disclosure of personal data**

1. Personal data processors and third parties may disclose personal data without the data subjects' consent in the following cases:

a) As required by the law;

b) As required for the sake of national security, social order and safety;

c) In the media for the sake of national defense and security, social order and safety, social morality, and public health;

d) On the media as required by the Law on Press without causing economic, reputational, spiritual or material damages to data subjects;

dd) As required by the law in emergency events that threaten life or seriously affect the health of the data subject or the public health.

2. Personal data processors and third parties shall immediately terminate the disclosure of personal data upon request by the data subject, except for the case specified in Clause 1 of this Article.

3. It is not allowed to disclose personal data of others in the following cases:

a) The data in question is sensitive personal data;

b) The disclosure may cause harm to the legitimate interests of data subjects.

4. The audio and/or video recording and processing of data obtained through the recording activities in public places by competent state agencies in cases stipulated by law is considered as being approved by the data subjects.

a) Agencies in charge of collection are obliged to notify data subjects in a way that they understand they are being audio or video recorded and they can stop recording if they so wish;

c) Notice is not required in the event of serving national defense and security, social order and safety, social morality, and public health.

**Article 7. Restricted access to personal data**

Personal data processors shall restrict access to personal data of those other than the data subjects in the following cases:

1. Such access may jeopardize national security, social order and safety.

2. Such access may affect the legitimate rights and interests of other organizations and individuals.

3. Disclosure or sharing of personal data with third parties in contravention of law.

4. Such access may affect the rights to privacy and freedom of others.

5. Such access may obstruct or affect the investigation and handling of regulatory violations.

**Article 8. Consent of the data subjects to personal data processing**

1. The data subjects' consent to the processing of their personal data shall only be valid if it is based on their informed discretion with regard to the following:

a) Types of personal data to be processed;

b) Purpose of personal data processing;

c) Relevant subjects with whom personal data is processed and shared;

d) Conditions for transferring or sharing personal data to a third party;

dd) Data subjects' legitimate rights related to the processing of their personal data.

2. Silence or non-response of data subjects shall not be interpreted as consent.

3. Data subjects may provide partial or conditional consent.

4. Data subjects' consent must be in a format that can be printed or copied in writing.

5. With regard to processing sensitive personal data, the data subjects must be informed that the data to be processed is sensitive personal data and their consent must be obtained in a format that can be printed or copied in writing.

6. Data subjects' consent shall be valid throughout the existence of the data subjects and for twenty years after the data subjects' death as for the activities of state agencies as prescribed by law, unless otherwise sanctioned by the data subjects.

7. Consent can be withdrawn by data subjects at any time.

8. In the event of a dispute, the responsibility for showing evidence of data subjects' consent rests with the personal data processors.

**Article 9. Processing of personal data of deceased data subjects**

1. Processing of personal data of deceased data subjects can only be done according to the will or written consent of the heirs (in the order of inheritance) as per regulatory provisions if there is any deviations from the agreement provided by the deceased data subjects to the personal data processors, provided that it complies with Clause 6, Article 8 of this Decree.

2. Clause 1 of this Article does not apply if the processed personal data contains only name, gender, date of birth, date of death, date of going missing and cause of death.

**Article 10. Processing of personal data without the data subject's consent**

1. Personal data may be processed without the data subjects' consent in the following cases:

a) As required by the law;

b) In support of national security, social order and safety;

c) As required by the law in emergency events that threaten life or seriously affect the health of the data subject or the public health;

d) In support of investigation and handling of regulatory violations;

dd) In compliance with specific provisions that explicitly allow the

processing of personal data without the data subject's consent under international agreements or treaties to which Vietnam is a signatory;

e) Process personal data for research or statistics purposes in accordance with Article 12 of this Decree.

2. Sharing of or access to personal data may be granted to a third party without the data subjects' consent in the following cases:

a) As required by the law or international agreements or treaties to which Vietnam is a signatory;

b) To protect the life, health or freedom of the data subjects;

c) Such sharing or access shall not affect the rights and interests of the data subjects and it is impossible to obtain the data subjects' consent;

d) Process personal data for research or statistics purposes in accordance with Article 12 of this Decree.

**Article 11. Notice provided to the data subject on personal data processing**

1. Data subjects must be informed of all activities related to processing personal data, except for the cases specified in Clause 3 of this Article and otherwise provided by law.

2. Contents of notice provided to the data subject on personal data processing:

a) Information on personal data processors;

b) Types of personal data to be processed and how;

c) Time and purpose of processing;

d) Types of personal data to be processed in special circumstances or special processing purposes may present a significant risk of harm;

dd) Rights and procedures for exercising the rights of data subjects;

e) Reliability rating in personal data protection performed by the Personal Data Protection Commission;

g) Information related to the transfer of personal data beyond the borders of Vietnamese territory;

h) Other information as prescribed.

3. Personal data processors shall not need to notify the processing of personal data in the following cases:

a) If the data subjects have provided full consent with the contents and activities of processing personal data;

b) If the processing of personal data is regulated by laws, international agreements and treaties;

c) Such processing shall not affect the rights and interests of the data subjects and it is impossible to notify the data subjects;

d) Process personal data for research or statistics purposes in accordance with Article 12 of this Decree.

**Article 12. Process personal data for research or statistics purposes**

1. The processing of personal data for research or statistics purposes in encrypted form does not require the data subjects' consent.

2. Before handing over personal data for processing in support of research or statistics purposes, personally identifiable information must be de-identified and replaced with a code. Decryption and decryption capabilities are only allowed to serve research or statistics purposes. Personal data processors shall designate a particular person in writing to grant access to information that can be decrypted.

3. Personal data processing results for research or statistics purposes cannot be synthesized into personally identifiable information of a specific data subject.

4. The processing of personal data for research or statistics purposes without the data subjects' consent requires the full implementation of the following measures:

a) Personal data protection commitments are in place;

b) Personal data protection measures are in place;

c) Personal data protection devices are in place;

d) There is a specialized department assigned to protect personal data;

dd) Registration to process sensitive personal data has been made with the Personal Data Protection Commission;

e) A written confirmation is obtained from the Personal Data Protection Commission verifying the conditions and compliance with the requirements specified at Points a, b, c, d, dd of this Clause.

**Article 13. Automated processing of personal data**

1. Automated processing of personal data may only be done during the process of contract executing or performance, provided that the data subjects are

informed and provide their consent to the automated data processing.

2. Data subjects must be informed of automated processing of personal data prior to execution.

3. The notification to data subjects must be made in a clear manner and easy to understand, including specific contents about the process and conditions for processing personal data.

**Article 14. Processing of children's personal data**

1. Principles of processing children's personal data

a) The processing of children's personal data shall always be done in accordance with the principle of protecting the rights and in the best interests of children;

b) Before processing any personal data of children, the data processors must verify the child's age and obtain the consent of their parent or guardian as prescribed.

2. When processing children's personal data, the personal data processors have the right to:

a) Correct inaccurate or misleading personal data;

b) Update inadequate personal data;

c) Update and handle outdated personal data;

d) Delete personal data that is no longer needed for the purpose of such data processing.

3. When performing the activities referred to in Clause 2 of this Article, the data processors shall take necessary steps to notify all parties concerned with the children's personal data.

4. Processing of children's personal data must be terminated in the following cases:

a) The collection has been completed or is no longer necessary for that purpose and when required by the data subject and guardian in accordance with the law;

b) Parents or guardians withdraw their consent for the processing of the children’s personal data;

c) At the request of a competent authority when there are sufficient grounds to prove that the processing of personal data affects children's legitimate rights and interests.

**Article 15. Accuracy of personal data**

Personal data processors shall be responsible for ensuring personal data is accurate and complete in the following cases:

1. Data subjects’ consent has been granted to personal data processing.

2. The authorized purpose of data processing is ensured.

**Article 16. Storage, deletion and destruction of personal data**

1. Personal data processors shall store personal data legally processed in an appropriate manner and take measures to prevent illegal processing of personal data.

2. Personal data processors shall stop storing, delete personal data and destroy means of storing personal data in the following cases:

a) The purposes of processing personal data registered or notified to data subjects are violated;

b) The retention of personal data is no longer necessary to the operation of the personal data processors;

c) Twenty years after the death of the data subject, unless otherwise decided by the data subject.

## Chapter III

## PERSONAL DATA PROTECTION MEASURES

**Article 17. Technical measures**

1. The personal data processors shall apply administrative, technical and physical measures to protect personal data to:

a) Ensure confidentiality, integrity and availability of personal data;

b) De-identify and encrypt information;

c) Store, copy, extract and protect personal data processing history of the personal data processors.

2. When processing personal data, the personal data processors must take measures to:

a) Prevent unauthorized access to devices used to process personal data;

b) Prevent unauthorized reading, copying, alteration or deletion of personal data;

c) Take statistics on the time, subjects and personal data recorded, changed or deleted or accessed;

d) Ensure the right to access, retrieve and process personal data of the authorized person;

dd) Take statistics on transmission, sharing and transfer of personal data by the following details: time, subject, type of data and form of storage;

e) Ensure that unauthorized reading, copying, alteration or deletion or destruction is not performed during the transfer or sharing of personal data via data communication devices and when transmitting via data carrier devices;

g) Take statistics on equipment and software for processing personal data, including: name, type, manufacturer's location and name; name, version and software manufacturer's name, and manufacturer's contact details.

**Article 18. Development of regulations on personal data protection**

1. Personal data processors shall develop and issue personal data protection documents that specify the implementation of the regulations herein.

2. Personal data processors shall designate a specialized department in charge of personal data protection, appoint personnel in charge of personal data protection and communicate information about the department and individual in charge of data protection to the Personal Data Protection Commission.

3. Personal data processors shall issue regulations on receiving and responding to complaints that may arise related to personal data protection.

**Article 19. Inspection and examination of personal data protection activities**

1. The Personal Data Protection Commission shall request the Director of the Department of Cyber Security and Hi-tech Crime Prevention and Control under the Ministry of Public Security to issue a decision on inspection and examination of personal data protection activities in accordance with their mandate. Members of the inspection team include members of the Personal Data

Protection Commission and competent authorities.

2. The inspection and examination of personal data protection shall be carried out no more than 02 times a year for any given agency or organization, unless there are grounds to determine that the agency, organization or individual violates the regulations on personal data protection.

**Article 20. Registration of processing of sensitive personal data**

1. Sensitive personal data must be registered with the Personal Data Protection Commission prior to processing.

2. Registration application for processing of sensitive personal data consists of:

a) An application for processing sensitive personal data, which consists of: name, registry or personally identifiable code, place of business, residence and other contact information of the the personal data processor; cited legal basis for processing personal data; purpose of processing personal data; types of personal data; types of subjects whose data is to be processed; sources of personal data; person or group authorized to transmit personal data; location where personal data is processed; conditions for the transfer of personal data to foreign countries; a detailed description of measures to protect personal data.

a) An impact assessment report for processing sensitive personal data, which consists of: a detailed description of the proposed processing activity, purpose of processing and the nature of the personal data being processed; assessment of potential harm to data subjects whose personal data is to be processed; measures to manage, minimize or eliminate such harm.

c) Documents and information related to the contents mentioned in the Application for processing sensitive personal data and the Impact assessment report for processing sensitive personal data.

3. The Personal Data Protection Commission shall process the registration for processing sensitive personal data within 20 working days from the date of receipt of the valid application. The Personal Data Protection Commission has the right to physically inspect the contents of the information stated in the application for processing sensitive personal data.

4. Personal data processors shall not need to register for processing sensitive personal data in the following cases:

a) Personal data is processed to serve the prevention, detection, investigation and handling of regulatory violations;

b) Personal data is processed to perform health care functions of public

health care and social security facilities in accordance with the law;

c) Personal data is processed to serve judicial functions of the Court;

d) Personal data is processed for research, filing or statistics purposes of a state agency or a research institution and verified by the Personal Data Protection Commission with regard to the following contents: A document is granted certifying the relevance of research, filing and statistics purposes according to the records; personal data has been de-identified; data subjects shall not be affected in any way;

dd) Other activities as prescribed by law.

**Article 21. Cross-border transfer of personal data**

1. Personal data of Vietnamese citizens can be transferred out of the border and territory of Vietnam when the following four conditions are fully satisfied:

a) Data subject's consent is granted for the transfer;

b) Original data is stored in Vietnam;

c) A document is granted proving that the recipient country, territory or a specific area within the recipient country or territory has issued regulations on personal data protection at a level equal to or higher than that specified in this Decree;

d) A written approval is obtained from the Personal Data Protection Commission.

2. The basis for the data protection agency to issue document on the cross-border transfer of personal data:

a) Effective protection of data subjects' rights under this Decree;

b) Commitment of the personal data processor when registering for the cross-border transfer of personal data;

c) Personal data protection measures shown by the personal data processor in the application.

3. Personal data may be transferred out of the territory of Vietnam without meeting the conditions specified in Clause 1 of this Article in the following cases:

a) Data subject's consent is granted for the transfer;

b) A written approval is obtained from the Personal Data Protection Commission;

c) There is commitment to protect personal data from the data processor;

d) There is commitment to apply personal data protection measures from the personal data processor.

4. The personal data processor that transfers data abroad must build a system to store data transfer history for 3 years, covering the following contents:

a) Time of transferring personal data abroad;

b) Receiver's identity, including name, address and contact form;

c) Type, quantity and sensitivity of the personal data transferred abroad;

d) Other contents as prescribed by the Personal Data Protection Authority.

5. The Personal Data Protection Commission shall periodically assess the Personal Data Processors' cross-border transfer of personal data once a year.

6. Cross-border transfers of personal data shall be terminated when either of the following events occurs:

a) The personal data processor or the recipient allows a large amounts of data to be abused or leaked;

b) It is impossible or difficult for the data subject to protect his legitimate interests;

c) The personal data processor or the recipient is incapable of protecting personal data.

7. Registration application for cross-border transfer of sensitive personal data consists of:

a) An application for cross-border transfer of personal data, which consists of: name, registry, place of business, residence and other contact information of the the personal data processor; cited legal basis for cross-border transfer of personal data; purpose of cross-border transfer of personal data; types of personal data to be transferred abroad; sources of personal data registered for cross-border transfer; location where cross-border transfer of personal data is registered; conditions for cross-border transfer of personal data; a detailed description of measures to protect personal data.

b) An impact assessment report for cross-border transfer of personal data, which consists of: a detailed description of the cross-border transfer of personal data, purpose of transferring personal data abroad; assessment of potential harm; measures to manage, minimize or eliminate such harm.

c) Documents related to the contents mentioned in the Application for processing sensitive personal data and the Impact assessment report for processing sensitive personal data.

8. The Personal Data Protection Commission shall process the registration for cross-border transfer of personal data within 20 working days from the date of receipt of the application. The Personal Data Protection Commission has the right to physically inspect the contents of the information stated in the application for cross-border transfer of personal data.

**Article 22. Handling of administrative violations of personal data processing**

1. A fine ranging from VND 50,000,000 to VND 80,000,000 shall be imposed for any of the following violations:

a) Violating regulations on the rights of the data subjects to personal data processing;

b) Violating regulations on personal data disclosure;

c) Violating regulations on restricted access to personal data;

d) Violating regulations on the consent of data subjects to personal data processing;

dd) Violating regulations on processing of personal data of deceased data subjects;

e) Violating regulations on processing of personal data in the absence of the consent of data subjects;

g) Violating regulations on notice provided to the data subject on personal data processing;

h) Violating regulations on personal data processing for research or statistics purposes;

i) Violating regulations on automated processing of personal data;

k) Violating regulations on processing children's personal data;

l) Violating regulations on the accuracy of personal data;

m) Violating regulations on storage, deletion and destruction of personal data.

2. A fine ranging from VND 80,000,000 to VND 100,000,000 shall be imposed for any of the following violations:

a) Failure to adopt technical measures and develop regulations on personal data protection;

b) Violating regulations on registration for processing sensitive personal data;

c) Violating regulations on cross-border transfer of personal data;

d) Second violation of the acts specified in Clause 1 of this Article.

3. A fine of up to 5% of the revenues of the violating personal data processor in Vietnam shall be imposed for the following acts:

a) Third violation of the acts specified in Clause 1 of this Article;

b) Second violation of the acts specified in Points a, b, and c, Clause 2 of this Article.

4. Additional sanctions:

a) Suspend the processing of personal data, from 01 month to 03 months, for violations specified in Clause 2 of this Article;

b) Revoke the written authorization to process sensitive personal data and transfer personal data out of the border and territory of Vietnam.

5. Remedial measures: Money gained from committing violations specified in Clauses 1 and 2 of this Article must be remitted to the competent authority.

6. The Director of the Department of Cyber Security and Hi-tech Crime Prevention and Control under the Ministry of Public Security shall be competent to sanction administrative violations in accordance with Clauses 1, 2, 3, 4, 5 of this Article.

## Chapter IV

## Personal Data Protection Commission

### Article 23. Personal Data Protection Commission

1. The Personal Data Protection Commission is an organization directly affiliated to the Government, based at the Department of Cyber Security and Hi-tech Crime Prevention and Control under the Ministry of Public Security. Members of the Personal Data Protection Commission include no more than 06

officers with professional qualifications and experience in personal data protection law, working on a part-time basis.

2. Personal Data Protection Commission shall have their own seal. The Chairman of Personal Data Protection Commission is the Director the Department of Cyber Security and Hi-tech Crime Prevention and Control under the Ministry of Public Security.

3. The Chairman and members of the Personal Data Protection Commission are appointed by the Ministry of Public Security upon endorsement by the Government.

**Article 24. Functions and duties of the Personal Data Protection Commission**

1. Implement activities to enhance personal data protection awareness.

2. Provide consulting, technical, administrative or other specialized services related to personal data protection.

3. Advise the Government on personal data protection issues.

4. Conduct research and promote educational activities related to personal data protection, including organizing and facilitating workshops and seminars on relevant topics, and assisting other organizations in carrying out such activities.

5. Manage technical cooperation and exchanges in the field of personal data protection with other organizations, including foreign data protection agencies, international or intergovernmental organizations, or organizations acting on behalf of the Government.

6. Protect the interests of data subjects, prevent any misuse of personal data, ensure compliance with the regulatory provisions and promote awareness about data protection.

7. Evaluate and rate the reliability of personal data protection of agencies and organizations and publish them on the National Personal Data Protection Portal.

8. Classify personal data and violations of personal data protection regulations.

9. Issue guidelines on personal data protection.

10. Monitor and evaluate developments in technology and commercial practices that can affect personal data protection.

11. Promote and conduct researches to innovate personal data protection.

12. Advise the Government and any other agency on the measures to protect personal data and ensure unified application and enforcement of

legislation on personal data protection.

13. Entitled to process personal data in support of the State activities, unless otherwise provided by law.

14. Appraise all personal data protection regulations of the Personal Data Processors prior to publication if related to the legitimate rights and interests of the data subjects. The scope of appraisal covers:

a) Contents and methods of notification to data subjects;

b) Personal data protection measures;

c) Measures related to the processing and storage of personal data;

d) Processing of personal data in the absence of the consent of data subjects;

dd) Processing of sensitive personal data;

e) Processing of children's personal data;

g) Exercise of any of the data owners' rights specified in this Decree;

h) Standards and means of protecting personal data;

i) Responsibility for personal data protection;

k) Cyber security protection measures for personal data;

l) De-identifying and anonymizing methods;

m) Methods of destroying or deleting personal data;

n) Impact assessment in collection, analysis, processing and storage of personal data;

o) Transfer of personal data beyond the borders of Vietnamese territory;

p) Process sensitive personal data for research, filing or statistics purposes;

q) Other issues related to personal data as prescribed by law.

15. Issue warning and coordinate to warn about risks and violations of personal data in accordance with law.

16. Receive registration for the processing of sensitive personal data and cross-border transfer of personal data.

17. The Director of the Department of Cyber Security and Hi-tech Crime Prevention and Control under the Ministry of Public Security is requested to carry out the following activities:

a) Inspect, examine, monitor and enforce regulations on personal data

protection;

b) Handle personal data breaches in accordance with the law;

c) Issue documents stating approval or disapproval of the registration for the processing of sensitive personal data and cross-border transfer of personal data;

d) Inspect and examine compliance with regulations on processing of sensitive personal data and cross-border transfer personal data;

dd) Settle complaints about personal data protection in accordance with this Decree;

e) Request personal data processors to change the way of collecting, processing and storing personal data in accordance with law;

g) Suspend, terminate or issue a written request to stop processing personal data if the agency or organization violates the regulations;

h) Suspend, terminate or revoke authorization granted to the personal data processors upon their violations of regulations on processing sensitive personal data and transferring personal data abroad.

## Chapter V

## RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS, AND INDIVIDUALS

### Article 25. Responsibilities of the Personal Data Protection Commission

1. Carry out the functions and duties specified in this Decree.

2. Formulate and promulgate criteria for assessing the reliability of personal data protection of agencies and organizations engaged in personal data processing.

3. Develop and operationalize a National Portal on personal data protection.

4. Receive and process registration for the processing of sensitive personal data and cross-border transfer of personal data.

5. Gather and publish a list of agencies and organizations engaged in personal data processing.

6. Organize workshops, conferences, and other activities on personal data protection.

7. Conduct annual review of personal data protection performance.

8. Monitor personal data protection in accordance with the law.

**Article 26. Responsibilities of relevant ministries and agencies**

1. Ministry of Public Security

a) The Ministry of Public Security shall assist the Government in exercising the unified state management of personal data protection;

b) Supervise and ensure the Personal Data Protection Commission operates in accordance with the prescribed functions and duties;

c) Investigate and handle regulatory violations on personal data protection.

2. The Ministry of Finance shall allocate recurrent funds for the operations of the Personal Data Protection Commission in accordance with the Law on State Budget and its guiding documents.

3. Ministries, Ministerial-level agencies, and Government’s agencies

a) Comply with regulations on personal data protection in this Decree;

b) Coordinate with the Personal Data Protection Commission on the list of organizations and individuals in charge of personal data protection;

c) Allocate funds for personal data protection in accordance with current budget management decentralization.

**Article 27. Responsibilities of People's Committees of provinces and centrally run cities**

1. Comply with regulations on personal data protection in this Decree.

2. Coordinate with the Personal Data Protection Commission on the list of organizations and individuals in charge of personal data protection;

3. Allocate funds for personal data protection in accordance with current budget management decentralization.

**Article 28. Responsibilities of concerned organizations and individuals**

1. Take measures to protect their personal data and be accountable for the accuracy of the personal data they provide.

2. Comply with regulations on personal data protection in this Decree.

3. Promptly notify the Personal Data Protection Commission of breaches to personal data protection.

4. Coordinate with the Ministry of Public Security and the Personal Data Protection Commission of breaches to personal data protection.

## Chapter VI

## IMPLEMENTATION PROVISIONS

### Article 29. Enforcement clause

This Decree shall take effect as of December 01, 2021.

### Article 30. Arrangements for implementation

1. The Minister of Public Security shall urge, inspect and guide the implementation of this Decree.

2. The Ministers, Heads of ministerial-level agencies, Heads of Governmental agencies, Presidents of People's Committees of central-affiliated cities and provinces are responsible for implementing this Decree./.

***Recipient(s):***
- Secretariat of the Party Central Committee;
- Prime Minister, Deputy Prime Ministers;
- Ministries, Ministerial-level agencies, Government's agencies;
- People's Councils and People's Committees of provinces and centrally-run cities;
- Office of the Party Central Committee and Party Committees;
- Office of the Party General Secretary;
- Office of the President;
- CEMA and Committees of the National Assembly;
- Office of the National Assembly;
- Supreme People's Court;
- Supreme People's Procuracy;
- Vietnam State Audit Office;
- National Financial Supervisory Commission;
- Central Committee of Vietnam Fatherland Front;
- Central agencies of socio-political organizations;
- Office of the Government: Minister, Chairman, Vice Ministers, Assistant to the Prime Minister, Departments;
- For filing; Admin., Administrative Procedure Control Dept. (3 copies).

**ON BEHALF OF GOVERNMENT**
**PRIME MINISTER**

**Nguyen Xuan Phuc**